702; and Matsui et. al, "Video-Steganography: How to Secretly Embed a Signature in a Picture," *IMA Intellectual Property Project Proceedings*, January 1994, Vol. 1, Issue 1, pp. 187-205.

[0019] There are various consortium research efforts underway in Europe on copyright marking of video and multimedia. A survey of techniques is found in "Access Control and Copyright Protection for Images (ACCOPI), WorkPackage 8: Watermarking," Jun. 30, 1995, 46 pages. A new project, termed TALISMAN, appears to extend certain of the ACCOPI work. Zhao and Koch, researchers active in these projects, provide a Web-based electronic media marking service known as Syscop.

[0020] Aura reviews many issues of steganography in his paper "Invisible Communication," Helskinki University of Technology, Digital Systems Laboratory, Nov. 5, 1995.

[0021] Sandford II, et al. review the operation of their May, 1994, image steganography program (BMPEMBED) in "The Data Embedding Method," SPIE Vol. 2615, Oct. 23, 1995, pp. 226-259.

[0022] A British company, Highwater FBI, Ltd., has introduced a software product which is said to imperceptibly embed identifying information into photographs and other graphical images. This technology is the subject of European patent applications 9400971.9 (filed Jan. 19, 1994), 9504221.2 (filed Mar. 2, 1995), and 9513790.7 (filed Jul. 3, 1995), the first of which has been laid open as PCT publication WO 95/20291.

[0023] Walter Bender at M.I.T. has done a variety of work in the field, as illustrate by his paper "Techniques for Data Hiding," Massachusetts Institute of Technology, Media Laboratory, January 1995.

[0024] Dice, Inc. of Palo Alto has developed an audio marking technology marketed under the name Argent. While a U.S. patent application is understood to be pending, it has not yet been issued.

[0025] Tirkel et al, at Monash University, have published a variety of papers on "electronic watermarking" including, e.g., "Electronic Water Mark," DICTA-93, Macquarie University, Sydney, Australia, December, 1993, pp. 666-673, and "A Digital Watermark," IEEE International Conference on Image Processing, Nov. 13-16, 1994, pp. 86-90

[0026] Cox et al, of the NEC Technical Research Institute, discuss various data embedding techniques in their published NEC technical report entitled "Secure Spread Spectrum Watermarking for Multimedia," December, 1995.

[0027] Möller et al. discuss an experimental system for imperceptibly embedding auxiliary data on an ISDN circuit in "Rechnergestützte Steganographie: Wie sie Funktioniert und warum folglich jede Reglementierung von Verschlusselung unsinnig ist," DuD, Datenschutz und Datensicherung, 18/6 (1994) 318-326. The system randomly picks ISDN signal samples to modify, and suspends the auxiliary data transmission for signal samples which fall below a threshold.

[0028] There are a variety of shareware programs available on the internet (e.g. "Stego" and "White Noise Storm") which generally operate by swapping bits from a to-be-concealed message stream into the least significant bits of an image or audio signal. White Noise Storm effects a randomization of the data to enhance its concealment.

BRIEF DESCRIPTION OF THE DRAWINGS

[0029] **FIG. 1** is a simple and classic depiction of a one dimensional digital signal which is discretized in both axes.

[0030] **FIG. 2** is a general overview, with detailed description of steps, of the process of embedding an "imperceptible" identification signal onto another signal.

[0031] **FIG. 3** is a step-wise description of how a suspected copy of an original is identified.

[0032] **FIG. 4** is a schematic view of an apparatus for pre-exposing film with identification information.

[0033] **FIG. 5** is a diagram of a "black box" embodiment.

[0034] **FIG. 6** is a schematic block diagram of the embodiment of FIG. 5.

[0035] **FIG. 7** shows a variant of the **FIG. 6** embodiment adapted to encode successive sets of input data with different code words but with the same noise data.

[0036] **FIG. 8** shows a variant of the **FIG. 6** embodiment adapted to encode each frame of a videotaped production with a unique code number.

[0037] FIGS. 9A-9C are representations of an industry standard noise second.

[0038] **FIG. 10** shows an integrated circuit used in detecting standard noise codes.

[0039] **FIG. 11** shows a process flow for detecting a standard noise code that can be used in the **FIG. 10** embodiment.

[0040] **FIG. 12** is an embodiment employing a plurality of detectors

[0041] **FIG. 13** shows an embodiment in which a pseudo-random noise frame is generated from an image.

[0042] **FIG. 14** illustrates how statistics of a signal can be used in aid of decoding.

[0043] **FIG. 15** shows how a signature signal can be preprocessed to increase its robustness in view of anticipated distortion, e.g. MPEG.

[0044] **FIGS. 16 and 17** show embodiments in which information about a file is detailed both in a header, and in the file itself.

[0045] FIGS. 18-20 show details relating to embodiments using rotationally symmetric patterns.

[0046] **FIG. 21** shows encoding "bumps" rather than pixels

[0047] FIGS. 22-26 detail aspects of a security card.

[0048] **FIG. 27** is a diagram illustrating a network linking method using information embedded in data objects that have inherent noise.

[0049] **FIGS. 27A and 27B** show a typical web page, and a step in its encapsulation into a self extracting web page object

Exhibit C-2
5,636,292

COPY

present invention is to avoid this reliance on expert testimony and to place the confidence in a match into simple "coin flip" vernacular, i.e., what are the odds you can call the correct coin flip 16 times in a row. Attempts to identify fragments of a fingerprint, document, or otherwise, exacerbate this issue of confidence in a judgment, where it is an object of the present invention to objectively apply the intuitive "coin flip" confidence to the smallest fragment possible. Also, storing unique fingerprints for each and every document or credit card magnetic strip, and having these fingerprints readily available for later cross-checking, should prove to be quite an economic undertaking. It is an object of this invention to allow for the "re-use" of noise codes and "snowy images" in the service of easing storage requirements.

Despite the foregoing and other diverse work in the field of identification/authentication, there still remains a need for a reliable and efficient method for performing a positive identification between a copy of an original signal and the original. Desirably, this method should not only perform identification, it should also be able to convey source-version information in order to better pinpoint the point of sale. The method should not compromise the inner quality of material which is being sold, as does the placement of localized logos on images. The method should be robust so that an identification can be made even after multiple copies have been made and/or compression and decompression of the signal has taken place. The identification method should be largely unerasable or "uncrackable." The method should be capable of working even on fractional pieces of the original signal, such as a 10 second "riff" of an audio signal or the "clipped and pasted" sub-section of an original image.

The existence of such a method would have profound consequences on piracy in that it could (a) cost effectively monitor for unauthorized uses of material and perform "quick checks"; (b) become a deterrent to unauthorized uses when the method is known to be in use and the consequences well publicized; and (c) provide unequivocal proof of identity, similar to fingerprint identification, in litigation, with potentially more reliability than that of fingerprinting.

In accordance with an exemplary embodiment of the invention, the foregoing and additional objects are achieved by embedding an imperceptible identification code throughout a source signal. In the preferred embodiment, this embedding is achieved by modulating the source signal with a small noise signal in a coded fashion. More particularly, bits of a binary identification code are referenced, one at a time, to control modulation of the source signal with the noise signal.

The copy with the embedded signal (the "encoded" copy) becomes the material which is sold, while the original is secured in a safe place. The new copy is nearly identical to the original except under the finest of scrutiny; thus, its commercial value is not compromised. After the new copy has been sold and distributed and potentially distorted by multiple copies, the present disclosure details methods for positively identifying any suspect signal against the original.

Among its other advantages, the preferred embodiments' use of identification signals which are global (holographic) and which mimic natural noise sources allows the maximization of identification signal energy, as opposed to merely having it present 'somewhere in the original material.' This allows the identification coding to be much more robust in the face of thousands of real world degradation processes and material transformations, such as cutting and cropping of imagery.

The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description thereof, which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a simple and classic depiction of a one dimensional digital signal which is discretized in both axes.

FIG. 2 is a general overview, with detailed description of steps, of the process of embedding an "imperceptible" identification signal onto another signal.

FIG. 3 is a step-wise description of how a suspected copy of an original is identified.

FIG. 4 is a schematic view of an apparatus for pre-exposing film with identification information in accordance with another embodiment of the present invention.

FIG. 5 is a diagram of a "black box" embodiment of the present invention.

FIG. 6 is a schematic block diagram of the embodiment of FIG. 5.

FIG. 7 shows a variant of the FIG. 6 embodiment adapted to encode successive sets of input data with different code words but with the same noise data.

FIG. 8 shows a variant of the FIG. 6 embodiment adapted to encode each frame of a videotaped production with a unique code number.

FIGS. 9A–9C are representations of an industry standard noise second that can be used in one embodiment of the present invention.

FIG. 10 shows an integrated circuit used in detecting standard noise codes.

FIG. 11 shows a process flow for detecting a standard noise code that can be used in the FIG. 10 embodiment.

FIG. 12 is an embodiment employing a plurality of detectors in accordance with another embodiment of the present invention.

FIG. 13 shows an embodiment of the present invention in which a pseudo-random noise frame is generated from an image.

FIG. 14 illustrates how statistics of a signal can be used in aid of decoding.

FIG. 15 shows how a signature signal can be preprocessed to increase its robustness in view of anticipated distortion, e.g. MPEG.

FIGS. 16 and 17 show embodiments of the invention in which information about a file is detailed both in a header, and in the file itself.

FIGS. 18–20 show details relating to embodiments of the present invention using rotationally symmetric patterns.

FIG. 21 shows how the invention can be practiced by encoding "bumps" rather than pixels.

FIGS. 22–26 detail aspects of a security card according to one embodiment of the present invention.

FIG. 27 is a flow chart illustrating processes according to various embodiment of the present invention.

FIG. 28 illustrates a diskette that can be used in accordance with the present invention.

DETAILED DESCRIPTION

In the following discussion of an illustrative embodiment, the words "signal" and "image" are used interchangeably to refer to both one, two, and even beyond two dimensions of